Operation ViceLeaker - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Operation ViceLeaker

Names	Operation ViceLeaker *(Kaspersky)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2018
Description	(Kaspersky) In May 2018, we discovered a campaign targeting dozens of mobile Android devices belonging to Israeli citizens. Kaspersky spyware sensors caught the signal of an attack from the device of one of the victims; and a hash of the APK involved (Android application) was tagged in our sample feed for inspection. Once we looked into the file, we quickly found out that the inner-workings of the APK included a malicious payload, embedded in the original code of the application. This was an original spyware program, designed to exfiltrate almost all accessible information. During the course of our research, we noticed that we were not the only ones to have found the operation. Researchers from Bitdefender also released an analysis of one of the samples in a blogpost. Although something had already been published, we decided to do something different with the data we acquired. The following month, we released a private report on our Threat Intelligence Portal to alert our clients about this newly discovered operation and began writing YARA rules in order to catch more samples. We decided to call the operation “ViceLeaker”, because of strings and variables in its code.
Observed	Sectors: Citizens. Countries: Israel.
Tools used	ViceLeaker.
Information	<https://securelist.com/fanning-the-flames-viceleaker-operation/90877/>

Last change to this card: 22 April 2020

Download this actor card in PDF or JSON format